**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF TEXAS**
**MARSHALL DIVISION**

| | |
|---|---|
| **MARKING OBJECT VIRTUALIZATION INTELLIGENCE, LLC,**<br><br>***Plaintiff,***<br><br>v.<br>**DELL INC.; F5 NETWORKS, INC.; AND SAP AMERICA, INC.,**<br><br>***Defendants.*** | **Civil Action No._____**<br><br>**JURY TRIAL DEMANDED** |

## COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Marking Object Virtualization Intelligence, LLC ("MOV Intelligence" or "Plaintiff"), by and through its attorneys, brings this action and makes the following allegations of patent infringement relating to U.S. Patent Nos.: 7,200,230 ("the '230 patent"); 6,802,006 ("the '006 patent"); 6,510,516 ("the '516 patent"); 7,650,504 ("the '504 patent"); 7,650,418 ("the '418 patent"); and 7,124,114 ("the '114 patent") (collectively, the "patents-in-suit" or the "MOV Intelligence Patents"). Defendant Dell Inc. ("Dell") infringes the '230 patent, the '006 patent, the '504 patent, and the '114 patent. Defendants Dell and SAP America, Inc. ("SAP") jointly infringe the '516 patent. Defendants Dell and F5 Networks, Inc. ("F5") jointly infringe the '418 patent. Dell, SAP and F5 Network's (collectively, the "Defendants") infringement violates the patent laws of the United States of America, 35 U.S.C. § 1 *et seq.*

## INTRODUCTION

1. MOV Intelligence and its wholly-owned subsidiary, MOV Global Licensing LLC ("MOV Global Licensing") pursues the reasonable royalties owed for Defendants' unauthorized use of patented groundbreaking technology both here in the United States and throughout

Europe. MOV Intelligence and its subsidiaries were assigned the rights to these patented technologies by Rovi Corporation ("Rovi").[1]

2. Rovi Corporation was a pioneer and leader in protecting computer technology, including digital rights management ("DRM") and digital watermarking systems. Rovi assigned MOV Intelligence rights to over 233 patents including many of John O. Ryan's, the founder of Rovi predecessor Macrovision, groundbreaking patents.[2]

## THE PARTIES

### MARKING OBJECT VIRTUALIZATION INTELLIGENCE, LLC

3. Marking Object Virtualization Intelligence, LLC ("MOV Intelligence") is a Texas limited liability company with its principal place of business located at 903 East 18th Street, Suite 217, Plano, Texas 75074. MOV Intelligence is committed to advancing the current state of DRM and watermarking technologies.

4. MOV Intelligence Global Licensing, LLC ("MOV Global Licensing") is a wholly-owned subsidiary of MOV Intelligence and assists in the licensing of MOV Intelligence's patents in territories outside the United States with a focus on the European Union (and the United Kingdom).[3] MOV Intelligence Global Licensing, LLC is a corporation organized under the laws of Delaware.

5. Rovi assigned the following patents to MOV Intelligence: U.S. Patent Nos. 7,299,209; 6,510,516; 6,802,006; 7,650,504; 6,813,640; 7,650,418; 7,200,230; 7,124,114; 6,381,367; 6,374,036; 6,360,000; 6,553,127; 6,701,062; 6,594,441; 7,764,790; 8,014,524; 6,931,536; and International Patent Nos. DE60047794; DE60148635.8; DE60211372.5; DE69901231.7-08; DK1047992; EP1047992; EP1303802; EP1332618; EP1444561;

[1] On April 29, 2016, Rovi Corporation acquired TiVo, Inc. The combined company operates under the name TiVo, Inc.

[2] *See* U.S. Patent Nos. 6,381,367; 7,764,790; 6,701,062; 8,014,524; German Patent Nos. DE60001837 and DE60001837D1; Chinese Patent No. CN1186941C; Canadian Patent No. CA2379992C; European Patent No. EP1198959B1; and Japanese Patent No. JP4387627B2.

[3] Wolfram Schrag, *EU-Patent steht auf der Kippe*, BR.COM NACHRICHTEN (August 2016).

ES1047992; FR1047992; FR1303802; FR1332618; FR1444561; GB1047992; GB1303802; GB1332618; GB1444561; GR3040059; IE1047992; IE1444561; IT1047992; NL1047992; NL1444561; PT1047992; and SE1047992.

6. MOV Intelligence has the right to sublicense the following international patent assets: AT1020077; AT1198959; AT1080584; ATE232346; AT1020077; AU729762; AU741281; AU753421; AU743639; AU714103; AU729762; AU2002351508; AU765747; AU2000263715; BE1020077; BE1198959; BE1020077; BE1080584; BE900498; BRPI 9812908-2; BR9709332.7; BRPI 9812908-2; CA2305254; CA2332546; CA2379992; CA2305254; CA2332548; CA2557859; CA2252726; CA2462679; CA2315212; CA2416304; CA2425115; CH1020077; CH1080584; CH900498; CH1020077; CH1047992; CNZL98809610.2; CNZL99806376.2; CNZL00811179.0; CNZL98809610.2; CNZL99806377.0; CNZL97194746.5; CNZL02820738.6; CNZL99802008.7; CNZL00819775.X; CNZL200510089437; DE69807102.608; DE60001837.7; DE69908352.4-08; DE69718907.4-08; DE69807102.608; DK1020077; DK1080584; DK1198959; DK1020077; DK900498; EP1020077; EP1198959; EP1080584; EP900498; EP1020077; ES1020077; ES1198959; ES1080584; ESES2191844; ES1020077; FI1020077; FI1080584; FI1020077; FI900498; FR1020077; FR1198959; FR1080584; FR900498; FR1020077; GB1020077; GB1198959; GB1080584; GB900498; GB1020077; GR3041381; GR3045620; GR3043304; GR3041381; HK1028696; HKHK1035625; HK1028696; HK1035282; HK1018562; HKHK1069234; HKHK1057115; HK1083653B; IE1020077; IE1198959; IE1020077; IE1080584; IE900498; IL135498; IL139543; IL148002; IL135498; IL139544; IN201442; IN220504; IN201442; IN207829; IT1020077; IT1080584; IT900498; IT1020077; JP4139560; JP4263706; JP4387627; JP4551617; JP4139560; JP4263706; JP3542557; JP4627809; JP4698925; JP4366037; JP4307069; KR374920; KR422997; KR761230; KR374920; KR362801; KR478072; KR689648; KR539987; KR752067; KR728517; KR593239; MX223464; MX231725; MX226464; MX223464; MX212991; MX214637; MX237690; MX240845; MYMY-123159-A; MYMY-123159-A; NL1020077; NL1198959; NL1080584;

NL900498; NL1020077; NZ503280; NZ507789; NZ503280; NZ532122; PT1010077; PT1198959; PT1080584; PT900498; PT1010077; RU2195084; RU2216121; RU2251821; RU2195084; RU2208301; RU2258252; SE1020077; SE1198959; SE1080584; SE900498; SE1020077; SG71485; SG76965; SG86547; SG76964; SG71485; TWNI117461; TWNI-124303; TWNI-130428; TWNI1600674; TWNI-162661; TWNI-202640; TWNI117461; TWNI-130754; and TWNI-184111.

**DELL INC.**

7. On information and belief, Dell Inc. is a Delaware corporation with its principal place of business at One Dell Way, Round Rock, Texas 78682. Dell is registered to do business in the State of Texas, and may be served through its registered agent Corporation Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701.

8. On information and belief, Dell employs thousands of employees and generates billions of dollars of revenue within the Eastern District of Texas. *See, e.g., Consolidated Work Station Computing, LLC v. Dell Inc., et al*., Case No. 6:10-cv-620, Dkt. No. 83 at 5 (E.D. Tex. Nov. 22, 2010) (denying Dell's motion to transfer, noting that "Dell Services is not a mere retail outlet or small services facility. Dell Services' 60-acre campus in Plano serves as its headquarters and as a workplace for over 2,000 Dell Services employees and the division itself generates near four billion dollars in annual revenue.").

**F5 NETWORKS, INC.**

9. On information and belief, F5 Networks, Inc. is a Washington corporation with its principal place of business at 401 Elliott Avenue West, Seattle, Washington 98119. F5 may be served through its registered agent CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. On information and belief, F5 is registered to do business in the State of Texas, and has been since at least November 30, 1998.

10. Dell and F5 Networks, in a joint enterprise, design, make, sell, offer to sell, import, and/or use a joint solution, the. F5 Big-IP for Dell DX Object Storage Platform (the "F5-

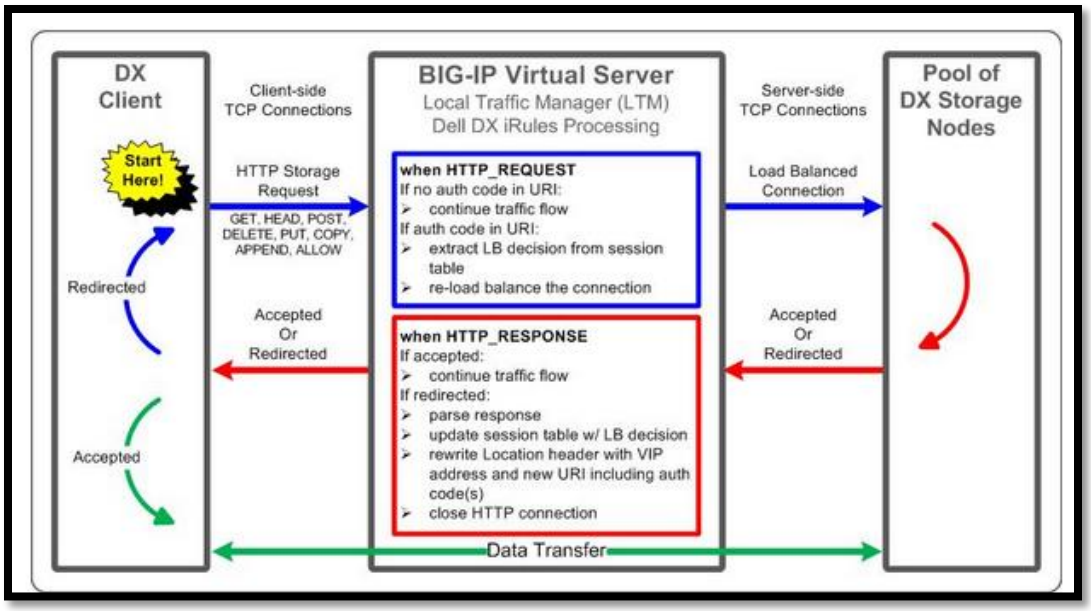
Dell Joint Solution"). F5 documentation describes the F5 Big-IP for Dell DX Object Storage Platform as a "joint solution."

> ***We are really excited about this new Dell | F5 joint solution*** that uses a simple iRules script to integrate BIG-IP and DX. This product combination greatly increases deployment flexibility for Dell's object storage platform and enables many of the ADC benefits that BIG-IP brings to the table.

Fred Johnson, *Deploying Dell's DX Object Storage? Then Check This Out*, F5 NETWORKS DEV CENTRAL (January 14, 2011) (Mr. Johnson is a strategic partner manager at F5 Networks) (emphasis added), available at: https://devcentral.f5.com/questions/deploying-dells-dx-object-storage-then-check-this-out

11. The "base functionality of the F5-Dell Joint Solution is provided by the DX iRules which is provided joints by Dell and F5. "The base functionality iRule provided by Dell and F5 supports local DX cluster access and it is a minimum requirement when using BIG-IP with DX. During configuration, you can copy and paste this script in to the BIG-IP virtual server set up."[4]

12. The below diagram from the Dell Tech Center website shows how the iRules functionality works in the F5-Dell Join Solution.




*BIG-IP for Dell DX Object Storage Platform*. DELL TECH CENTER WEBSITE (last visited September 2016), available at: http://en.community.dell.com/techcenter/networking/w/wiki/2592

[4] *BIG-IP for Dell DX Object Storage Platform*. DELL TECH CENTER WEBSITE (last visited September 2016), available at: http://en.community.dell.com/techcenter/networking/w/wiki/2592

13. Dell is the largest reseller of F5 Products. "As the largest reseller of F5 solutions, Dell works with F5 to improve the purchase process of F5 products through Dell."[5] The Dell-F5 Joint Solution is described by Dell as offered "strategic control of cloud storage."

> The Dell DX Object Storage Platform goes beyond traditional object storage by deploying the F5 BIG-IP as a strategic control point. This storage configuration extends multi-tenancy and security functions to the network while providing deployment options designed to be extremely flexible, manageable, scalable, and easily accessed.

Gene Chesser, Eric Dey, and Fred Johnson, *Simplifying Data Management Through Agile and Secure Cloud Storage*, DELL POWER SOLUTIONS, 2011 Issue 1 (2011).

14. As described in Count V, below, Defendants' F5-Dell Joint Solution infringes the '418 patent. Defendants are properly joined in this action pursuant to 35 U.S.C. § 299.

**SAP AMERICA, INC.**

15. On information and belief, SAP America, Inc. is a Delaware corporation with its principal place of business at 3999 West Chester Pike, Newtown Square, Pennsylvania 19073. SAP may be served through its registered agent CT Corporation System 1999 Bryan Street, Suite 900, Dallas, Texas 75201. On information and belief, SAP is registered to do business in the State of Texas, and has been since at least June 15, 1992.

16. On information and belief, SAP conducts business operations throughout the State of Texas, including at its facilities at 5212 N. O'Connor Boulevard, Suite 800, Irving, Texas 75039, and 2601 Westheimer Road, Suite C250 Houston, Texas 77098.

17. Dell and SAP, in a joint enterprise, design, make, sell, offer to sell, import, and/or use a joint solution, the Dell SAP HANA Solution (incorporating the Dell PowerEdge R920 platform).

> Dell and SAP collaborated to create an optimally configured SAP HANA solution that includes a hardware appliance, pre-loaded software, and a full range of services. This solution is reliable, scalable, and offered in multiple configurations

[5] *Dell and F5 Networks Partnership Program*, DELL AND F5 DATA SHEET (last visited September 2016); available at: www.f5.com/pdf/solution-center/dell-f5-partnership-old.pdf

> to address specific business needs. Dell's end-to-end solutions give an organization access to the full power of SAP HANA.

DELL SAP HANA SOLUTION OVERVIEW AND SIZING GUIDE at 5 (2012).

18. The Dell SAP HANA Solution is described in Dell's documentation as being an "end-to-end" solution that is based on Dell and SAP's unique partnership.

> Dell and SAP have teamed up to offer optimally configured SAP HANA solutions that include a hardware appliance, preloaded software and a full range of services. Pairing Dell's enterprise class products and expert services with SAP HANA allows users to execute business analytics, performance management, and operations in a single system. This end-to-end solution gives enterprise customers cost-effective, optimized in-memory computing capabilities that increase availability and reduce risk.

DELL VALIDATED SYSTEMS FOR SAP HANA at 2 (2014) (the documentation from Dell goes onto state that "With Dell's SAP Hana appliance . . . The Dell Solution offers: Every appliance configuration is based on the Dell PowerEdge R230 Platform, providing a consistent experience.").

19. Further, Dell and SAP have jointly developed the Dell SAP HANA Solution. "For more than a decade, Dell has collaborated with SAP to deliver hundreds of SAP solutions across many industries."[6] The same document descrines the Dell SAP HANA Solution as a "highly-tuned integration."[7]

20. As described in Count III, below, Defendants' Dell SAP HANA Solution infringes the '516 patent. Defendants are properly joined in this action pursuant to 35 U.S.C. § 299.

## JURISDICTION AND VENUE

21. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

22. Upon information and belief, this Court has personal jurisdiction over Defendants in this action because Defendants have committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the

[6] *Dell's SAP HANA™ Appliance*, DELL DATASHEET AT 1 (2012)
[7] *Id.*

exercise of jurisdiction over Defendants would not offend traditional notions of fair play and substantial justice. Defendants, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), have committed and continue to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit.

23. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Upon information and belief, Defendants have transacted business in the Eastern District of Texas and have committed acts of direct and indirect infringement in the Eastern District of Texas.

## MOV INTELLIGENCE'S LANDMARK INVENTIONS

24. The groundbreaking inventions in DRM and digital watermarking taught in the patents-in-suit were pioneered by Rovi. Rovi, established in 1983 under the name Macrovision, was a trailblazing technology company focused on inventing and bringing to market fundamental technologies designed to allow producers and distributors of film and music to widely distribute their products while simultaneously protecting their art from unauthorized copying.[8] Macrovision's copy protection technology became so important to content creators that Congress specifically regulated the manufacture and sale of technology that was incompatible with Macrovision's copy protection technology. *See* 17 U.S.C. § 1201(k)(1) ("unless such recorder conforms to the automatic gain control copy control technology").[9] Rovi broadened its focus to include copy protection and DRM for other media,[10] including computer executables, firmware, operating system images, watermarking, and encryption.

[8] Aljean Harmetz, *Cotton Club Cassettes Coded to Foil Pirates*, N.Y. TIMES (April 24, 1985).

[9] *See also* David Nimmer, *Back from the Future: A Proleptic Review of the Digital Millennium Copyright Act*, 16 BERKELEY TECH. L.J. 855, 862 (2001) (The DMCA "contains a welter of corporation-specific features, relating to Macrovision Corp. The features in question relate to section 1201's controls on consumer analog devices.") (citations omitted).

[10] *See* Michael Arnold et al., TECHNIQUES AND APPLICATIONS OF DIGITAL WATERMARKING AND CONTENT PROTECTION 203 (2002) (Describing Rovi's Cactus Data Shield product which by 2002 had been used in over 100 million compact discs. "This scheme [Rovi Cactus Data Shield] operates by inserting illegal data values instead of error-correcting codes."); *see also Rovi*

25. MOV Intelligence's patent portfolio, which includes more than 233 issued patents worldwide, is a direct result of Rovi's substantial investment in research and development. The asserted MOV Intelligence patents are reflective of this history of innovation, embodying a number of firsts in the development of DRM and watermarking technologies.

26. MOV Intelligence long-term financial success depends in part on its ability to establish, maintain, and protect its proprietary technology through patents. Defendant's infringement presents significant and ongoing damage to MOV Intelligence's business. Defendants, in an effort to expand their product bases and profit from the sale of patented technology, have chosen to incorporate MOV Intelligence's fundamental technology without a license or payment.

## THE ASSERTED PATENTS

### U.S. PATENT NO. 7,200,230

27. U.S. Patent No. 7,200,230 (the "'230 patent"), entitled "System and Method for Controlling and Enforcing Access Rights to Encrypted Media," was filed January 15, 2001, and claims priority to April 6, 2000. MOV Intelligence is the owner by assignment of the '230 patent. A true and correct copy of the '230 patent is attached hereto as Exhibit A. The '230 patent claims specific methods and systems for extending the capabilities of rights controlled access media systems. Further, the system and methods provide for designation and authentication of the identity of the data processor upon/through which a data object is to be used. The system and methods also provide\ for encryption of a data object and its associated rules such that only a designated data processor can decrypt and use the data object. The system and methods further provide for designation and authentication of the identity of a user by whom

*SafeDisc Copy Protection Overview*, MACROVISION CORPORATION DATASHEET at 2 (1999) ("SafeDisc incorporates a unique authentication technology that prevents the re-mastering of CD-ROM titles and deters attempts to make unauthorized copies. The SafeDisc authentication process ensures that consumers will only be able to play original discs. The user is forced to purchase a legitimate copy."); Kirby Kish, MACROSAFE SYSTEM: A SOLUTION FOR SECURE DIGITAL MEDIA DISTRIBUTION at 7 (January 2002) (showing the architecture of the MacroSafe system and use of a DRM Server and Key Escrow Server).

the data object is to be used. The system and methods also provide for encryption of a data object and its associated rules such that only a designated user can decrypt and use the data object.

28. The ‘230 patent has been cited by over 180 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘230 patent as relevant prior art:

- International Business Machines Corporation
- Qualcomm Incorporated
- Autodesk, Inc.
- NTT Docomo, Inc.
- Hitachi, Ltd.
- Koninklijke Phillips Electronics N.C.
- Hewlett-Packard Development Company L.P.
- Time Warner Cable, Inc.
- Cisco Systems, Inc.
- Blackberry Limited
- Arris Enterprises, Inc.
- Meshnetworks, Inc.
- Google, Inc. (now Alphabet, Inc.)
- Oracle Corporation
- General Instrument Corporation
- Symantec Corporation
- Siemens Aktiengesellschaft
- AT&T, Inc.
- Nokia Corporation
- Verizon Communications, Inc.
- Voltage Security, Inc.
- Scientific-Atlanta, Inc. (subsequently acquired by Cisco Systems, Inc.)
- Telefonaktiebolaget LM Ericsson

29. The ‘230 patent claims a technical solution to a problem unique to the transmission of digital information over a network – providing systems and methods for extending the capabilities of rights controlled access to digital content using three layers of encryption.

**U.S. PATENT NO. 6,802,006**

30. U.S. Patent No. 6,802,006 (the "'006 patent"), entitled "System and Method of Verifying the Authenticity of Dynamically Connectable Executable Images," was filed on July 22, 1999, and claims priority to January 15, 1999. MOV Intelligence is the owner by assignment of the '006 patent. A true and correct copy of the '006 patent is attached hereto as Exhibit B. The '006 patent claims specific methods and systems for verifying the authenticity of executable images. The system includes a validator that determines a reference digital signature for an executable image using the contents of the executable image excluding those portions of the executable that are fixed-up by a program loader. The validator then, subsequent to the loading of the executable image, determines an authenticity digital signature to verify that the executable image has not been improperly modified.

31. The '006 patent has been cited by over 85 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '006 patent as relevant prior art:

- Intertrust Technologies Corporation
- International Business Machines Corporation
- Intel Corporation
- Microsoft Corporation
- Check Point Software Technologies, Inc.
- Nokia Corporation
- Ipass, Inc.
- Nytell Software LLC
- Amazon Technologies, Inc.
- Panasonic Corporation
- Matsushita Electric Ind. Co. Ltd.
- NXP B.V. (now Cisco Systems, Inc.)
- Intel Corporation
- Hewlett-Packard Development Company, L.P.
- Apple, Inc.
- Lockheed Martin Corporation
- Symantec Corporation
- Zone Labs, Inc.

32. The '006 patent claims a technical solution to a problem unique to computer systems: verifying and authenticating executable images.

**U.S. PATENT NO. 6,510,516**

33. U.S. Patent No. 6,510,516 (the "'516 patent"), entitled "System and Method for Authenticating Peer Components," was filed on January 15, 1999, and claims priority to January 16, 1998. MOV Intelligence is the owner by assignment of the '516 patent. A true and correct copy of the '516 patent is attached hereto as Exhibit C. The '516 patent claims specific methods and systems for controlling the usage of data objects in component object systems. According to the invention, each data object includes a peer list that defines one or more peer data objects that are required by the data object. Upon receipt of a data object, the system verifies the integrity of the data object. Further, the system identifies the integrity of the peer data objects.

34. The '516 patent family has been cited by over 108 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '516 patent as relevant prior art:

- America Online, Inc.
- LG Electronics, Inc.
- Microsoft Corporation
- Samsung Electronics Co., Ltd.
- First Data Corporation
- International Business Machines Corporation
- Pixar, Inc. (now a subsidiary of the Walt Disney Company)
- Adobe Systems Incorporated
- The Western Union Company
- Verizon Communications, Inc.
- JPMorgan Chase & Co.
- Electronics and Telecommunications Research Institute (ETRI)
- Siemens Medical Solutions USA, Inc.

**U.S. PATENT NO. 7,650,504**

35. U.S. Patent No. 7,650,504 (the "'504 patent"), entitled "System and Method of Verifying the Authenticity of Dynamically Connectable Executable Images," was filed on August 23, 2004, and claims priority to July 22, 1999. MOV Intelligence is the owner by assignment of the '504 patent. A true and correct copy of the '504 patent is attached hereto as Exhibit D. The '504 patent claims specific methods and systems for verifying the authenticity of executable images. The systems and methods taught in the '504 patent incorporate a validator

that determines a reference digital signature for an executable image using the contents of the executable image excluding those portions of the executable that are fixed-up by a program loader. The validator then, subsequent to the loading of the executable image, determines an authenticity digital signature to verify that the executable image has not been improperly modified. In addition, the validator ensures that each of the pointers in the executable image have not been improperly redirected.

36. The '504 patent and its underlying application have been cited by over 30 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '504 patent as relevant prior art:

- Qualcomm Incorporated
- Intel Corporation
- Micro Beef Technologies, Ltd
- Microsoft Corporation
- Apple, Inc.
- Symantec Corporation
- Samsung Electronics Co., Ltd.
- Cybersoft Technologies, Inc.
- Electronics and Telecommunications Research Institute (ETRI)

37. The '504 patent claims a technical solution to a problem unique to the transmission of digital information over a network: verifying the identity of a software application in a dynamic loading environment. In particular, the system determines whether a software application that has been dynamically connected to another data object has been tampered with subsequent to the execution of the software application.

**U.S. PATENT NO. 7,650,418**

38. U.S. Patent No. 7,650,418 (the "'418 patent"), entitled "System and Method for Controlling the Usage of Digital Objects," was filed on August 26, 2004, and claims priority to December 8, 1998. MOV Intelligence is the owner by assignment of the '418 patent. A true and correct copy of the '418 patent is attached hereto as Exhibit E. The '418 patent claims specific methods and systems for controlling the usage of digital objects wherein control rights associated with a digital data object activate an external control object and an intercept application to

intercept and monitor communications between a hosting application and a document server application associated with the creation of the digital data object. The '418 patent teaches the use of intercepting and monitoring functions without affecting or changing the hosting application or the document server application. The external control object activates an intercept application which mimics the functions of the document server application and performs user actions on the digital data object as authorized by the external control object according to the control rights associated with the digital object. By intercepting and monitoring user actions on a digital data object, the invention can control access and use of the digital data object.

39. The '418 patent family has been cited by over 47 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '418 patent as relevant prior art:

- Google, Inc.
- Fisher-Rosemount Systems, Inc.
- Knoa Software, Inc.
- Securewave S.A.
- International Business Machines Corporation
- Ab Initio Technology LLC
- The Invention Science Fund I, LLC
- Searete LLC
- Microsoft Corporation

40. The '418 patent claims a technical solution to a problem unique to the transmission of digital information over a network: reliably controlling the usage of digital objects wherein the system and/or methods intercept the communication between two applications communicating over a computer network.

**U.S. PATENT NO. 7,124,114**

41. U.S. Patent No. 7,124,114 (the "'114 patent"), entitled "Method and Apparatus for Determining Digital A/V Content Distribution Terms Based on Detected Piracy Levels," was filed on November 9, 2000. MOV Intelligence is the owner by assignment of the '114 patent. A true and correct copy of the '114 patent is attached hereto as Exhibit F. The '114 patent claims specific methods and systems for distributing copyrighted material over a computer network.

Specifically, the ‘114 patent teaches the providing of protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to the prospective recipient; and providing or withholding a copy of the protected material to the prospective recipient in accordance with the terms. The ‘114 patent also discloses the use of a first set of program code which serves to ascertain terms for providing a protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to the prospective recipient. The first set of program code also serves to provide or withhold a copy of the protected material to or from the prospective recipient in accordance with the terms.

42. The ‘114 patent family has been cited by over 39 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘114 patent as relevant prior art:

- Google, Inc.
- NBCUniversal Media, Inc.
- Digimarc Corporation
- Hewlett-Packard Development Company, L.P.
- Aigo Research Institute of Image Computing Co., Ltd.
- AT&T Intellectual Property I, L.P.
- General Electric Company
- The Nielsen Company (US), LLC
- Sca Ipla Holdings, Inc.
- Thomson Licensing, Inc.
- Fujitsu Limited

43. The ‘114 patent claims a technical solution to a problem unique to the transmission of digital information over a network: preventing the unauthorized copying of digital content. The patent teaches the use of a server that manages access to content according to terms determined from information stored in a database of prior unauthorized copying attributed to that recipient.

**COUNT I**
**INFRINGEMENT OF U.S. PATENT NO. 7,200,230**

44. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

45. Dell designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for digital rights management.

46. Dell designs, makes, sells, offers to sell, imports, and/or uses the Dell Cloud Manager v11 system (the "Dell CM System").

47. Dell designs, makes, sells, offers to sell, imports, and/or uses the Dell Data Protection system, including but not limited to Dell Data Protection – Encryption Enterprise Edition, Dell Data Protection – Cloud Edition, Dell Data Protection – Encryption, and Dell Data Protection – Mobile Edition (collectively, the "Dell DP System")

48. The Dell CM System and Dell DP System (collectively, the "Dell '230 Product(s)") include digital rights management technology.

49. On information and belief, one or more Dell subsidiaries and/or affiliates use the Dell '230 Products in regular business operations.

50. On information and belief, one or more of the Dell '230 Products enable associating a user program key with a user program configured to run on a user data processor.

51. On information and belief, the Dell '230 Products are available to businesses and individuals throughout the United States.

52. On information and belief, the Dell '230 Products are provided to businesses and individuals located in the Eastern District of Texas.

53. On information and belief, the Dell '230 Products enable determining whether the use of the data object is to be restricted to a particular user data processor.

54. On information and belief, the Dell '230 Products comprise a system wherein a machine key device is associated with the particular user data processor. Further, the machine

key device is accessible by the user program, and the machine key device maintains a portion of a machine key.

55. On information and belief, the Dell '230 Products enable encrypting a data object so the decryption of a first secure layer and a second secure layer of the encrypted data object requires the user program key and the machine key.

56. On information and belief, the Dell '230 Products enable determining whether the use of the data object is to be restricted to a particular user.

57. On information and belief, the Dell '230 Products provide for the designation and authentication of the identity of a user by whom the data object is to be used.

58. On information and belief, the Dell '230 Products enable associating a user key device with the particular user. Further, the Dell '230 Products enable the user key device to be made accessible by the user program. And, the user key device maintains a portion of a user key.

59. On information and belief, the Dell '230 Products contain functionality for encrypting a data object so the decryption of a third secure layer of the encrypted data object requires the user key.

60. On information and belief, the Dell '230 Products contain functionality wherein the third key used by the system for managing digital rights is the media access controller (MAC) address of the user data processor.

61. On information and belief, the Dell '230 Products provide for encryption of a data object so only a designated data processor can decrypt and use the data object.

62. On information and belief, the Dell '230 Products enable user specific digital rights management authorization and access.

63. On information and belief, Dell has directly infringed and continues to directly infringe the '230 patent by, among other things, making, using, offering for sale, and/or selling digital content protection technology, including but not limited to the Dell '230 Products, which

include infringing digital rights management technology. Such products and/or services include, by way of example and without limitation, the Dell CM System and the Dell DP System.

64. By making, using, testing, offering for sale, and/or selling digital rights management products and services, including but not limited to the Dell '230 Products, Dell has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '230 patent, including at least claim 39, pursuant to 35 U.S.C. § 271(a).

65. On information and belief, Dell also indirectly infringes the '230 patent by actively inducing infringement under 35 USC § 271(b).

66. On information and belief, Dell had knowledge of the '230 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Dell knew of the '230 patent and knew of its infringement, including by way of this lawsuit.

67. On information and belief, Dell intended to induce patent infringement by third-party customers and users of the Dell '230 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Dell specifically intended and was aware that the normal and customary use of the accused products would infringe the '230 patent. Dell performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '230 patent and with the knowledge that the induced acts would constitute infringement. For example, Dell provides the Dell '230 Products that have the capability of operating in a manner that infringe one or more of the claims of the '230 patent, including at least claim 39, and Dell further provides documentation and training materials that cause customers and end users of the Dell '230 Products to utilize the products in a manner that directly infringe one or more claims of the '230 patent. By providing instruction and training to customers and end-users on how to use the Dell '230 Products in a manner that directly infringes one or more claims of the '230 patent, including at least claim 39, Dell specifically intended to induce infringement of the '230 patent. On information and belief, Dell engaged in such inducement to promote the sales of the Dell '230 Products, e.g., through Dell user manuals, product support, marketing materials, and

training materials to actively induce the users of the accused products to infringe the ‘230 patent. Accordingly, Dell has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘230 patent, knowing that such use constitutes infringement of the ‘230 patent.

68. The ‘230 patent is well-known within the industry as demonstrated by the over 180 citations to the ‘230 patent family in published patents and published patent applications assigned to technology companies and academic institutions. Several of Dell’s competitors have paid considerable licensing fees for their use of the technology claimed by the ‘230 patent. In an effort to gain an advantage over Dell’s competitors by utilizing the same licensed technology without paying reasonable royalties, Dell infringed the ‘230 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

69. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘230 patent.

70. As a result of Dell’s infringement of the '230 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Dell’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Dell together with interest and costs as fixed by the Court.

## COUNT II
## INFRINGEMENT OF U.S. PATENT NO. 6,802,006

71. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

72. Dell designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for determining the authenticity of an executable image.

73. Dell designs, makes, sells, offers to sell, imports, and/or uses the Dell KACE K1000 Systems Management Appliance 6.4.120822; Dell KACE K1000 Systems Management Appliance 6.4.120756; Dell KACE K1000 Systems Management Appliance 6.4; Dell KACE

K1000 Systems Management Appliance 6.3; Dell KACE K1000 Systems Management Appliance 6.2.109330; Dell KACE K1000 Systems Management Appliance 6.2.109329; Dell KACE K1000 Systems Management Appliance 6.0.101863; Dell KACE K1000 Systems Management Appliance 5.590545; Dell KACE K1000 Systems Management Appliance 5.4.76847; and the Dell KACE K1000 Systems Management Appliance 5.4.70402 (the "Dell '006 Product(s)").

74. On information and belief, one or more Dell subsidiaries and/or affiliates use the Dell '006 Products in regular business operations.

75. On information and belief, one or more of the Dell '006 Products include authentication technology.

76. On information and belief, one or more of the Dell '006 Products enable authenticating the identity of a software application in a dynamic loading environment. In particular, the Dell '006 Products determine whether an executable image has been dynamically connected to another data object that has been tampered with subsequent to the execution of the software application.

77. On information and belief, the Dell '006 Products are available to businesses and individuals throughout the United States.

78. On information and belief, the Dell '006 Products are provided to businesses and individuals located in the Eastern District of Texas.

79. On information and belief, the Dell '006 Products enable identifying one or more locations within the executable image, each of the identified locations being modified by a program loader.

80. On information and belief, the Dell '006 Products comprise a system wherein a reference digital signature is generated based on an executable image.

81. On information and belief, the Dell '006 Products generate a reference digital signature that excludes one or more locations in an executable image.

82. On information and belief, the Dell '006 Products are capable of storing the reference digital signature on a computer network.

83. On information and belief, the Dell '006 Products comprise systems and methods wherein an authenticity digital signature is generated based on an executable image.

84. On information and belief, the Dell '006 Products comprise systems and methods that generate an authenticity digital signature that excludes one or more locations in an executable image.

85. On information and belief, the Dell '006 Products comprise systems and methods that determine whether the authenticity digital signature matches the reference digital signature.

86. On information and belief, the Dell '006 Products contain functionality that generates a warning if the reference digital signature does not match the authenticity digital signature.

87. On information and belief, the Dell '006 Products contain functionality wherein the digital signature is generated based on a first and second point in time. For example, one or more of the Dell '006 Products generate a reference digital signature at a first point in time. Subsequently, an authenticity digital signature is generated (at a second point in time).

88. On information and belief, the Dell '006 Products comprise a system and method that generates a digital signature based on a hash value. Specifically, the reference digital signature that is generated by the Dell '006 Products at a first point in time is based on a hash value. Later the authenticity digital signature is also generated based on a hash function that is used to check data integrity.

89. On information and belief, the Dell '006 Products comprise a system and method that can verify the identity a computer application.

90. On information and belief, the Dell '006 Products enable the detection of corrupted data in a computer image.

91. On information and belief, the Dell '006 Products enable the verification of the integrity of software images.

92. On information and belief, Dell has directly infringed and continues to directly infringe the ‘006 patent by, among other things, making, using, offering for sale, and/or selling content protection technology, including but not limited to the Dell ‘006 Products, which includes technology for verifying the authenticity of a software image. Such products and/or services include, by way of example and without limitation, the Dell KACE K1000 Systems Management Appliance 6.4.120822; Dell KACE K1000 Systems Management Appliance 6.4.120756; Dell KACE K1000 Systems Management Appliance 6.4; Dell KACE K1000 Systems Management Appliance 6.3; Dell KACE K1000 Systems Management Appliance 6.2.109330; Dell KACE K1000 Systems Management Appliance 6.2.109329; Dell KACE K1000 Systems Management Appliance 6.0.101863; Dell KACE K1000 Systems Management Appliance 5.590545; Dell KACE K1000 Systems Management Appliance 5.4.76847; and the Dell KACE K1000 Systems Management Appliance 5.4.70402.

93. By making, using, testing, offering for sale, and/or selling verification and authentication products and services, including but not limited to the Dell ‘006 Products, Dell has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the ‘006 patent, including at least claims 1, 3, 14, and 15, pursuant to 35 U.S.C. § 271(a).

94. On information and belief, Dell also indirectly infringes the ‘006 patent by actively inducing infringement under 35 USC § 271(b).

95. On information and belief, Dell had knowledge of the ‘006 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Dell knew of the ‘006 patent and knew of its infringement, including by way of this lawsuit.

96. On information and belief, Dell intended to induce patent infringement by third-party customers and users of the Dell ‘006 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Dell specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘006 patent. Dell performed the acts that constitute

induced infringement, and would induce actual infringement, with knowledge of the ‘006 patent and with the knowledge that the induced acts would constitute infringement. For example, Dell provides the Dell ‘006 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘006 patent, including at least claims 1, 3, 14, and 15, and Dell further provides documentation and training materials that cause customers and end users of the Dell ‘006 Products to utilize the products in a manner that directly infringe one or more claims of the ‘006 patent. By providing instruction and training to customers and end-users on how to use the Dell ‘006 Products in a manner that directly infringes one or more claims of the ‘006 patent, including at least claims 1, 3, 14, and 15, Dell specifically intended to induce infringement of the ‘006 patent. On information and belief, Dell engaged in such inducement to promote the sales of the Dell ‘006 Products, *e.g.*, through Dell user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘006 patent. Accordingly, Dell has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘006 patent, knowing that such use constitutes infringement of the ‘006 patent.

97. The ‘006 patent is well-known within the industry as demonstrated by the over 85 citations to the ‘006 patent in issued patents and published patent applications assigned to technology companies and academic institutions. Several of Dell’s competitors have paid considerable licensing fees for their use of the technology claimed by the ‘006 patent. In an effort to gain an advantage over Dell’s competitors by utilizing the same licensed technology without paying reasonable royalties, Dell infringed the ‘006 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

98. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘006 patent.

99. As a result of Dell’s infringement of the '006 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Dell’s

infringement, but in no event less than a reasonable royalty for the use made of the invention by Dell together with interest and costs as fixed by the Court.

**COUNT III**
**INFRINGEMENT OF U.S. PATENT NO. 6,510,516**

100. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

101. Dell and SAP, in a joint enterprise, design, make, use, sell, and/or offer for sale in the United States products and/or services for authenticating peer data objects.

102. Dell and SAP, in a joint enterprise, design, make, sell, offer to sell, import, and/or use a joint solution, the Dell SAP HANA Solution (incorporating the Dell PowerEdge R920 platform) (the "Dell-SAP '516 Product(s)") pursuant to ongoing contractual agreements between Dell and SAP.

103. On information and belief, one or more of Dell and SAP's subsidiaries and/or affiliates use the Dell-SAP '516 Products in regular business operations.

104. On information and belief, one or more of the Dell-SAP '516 Products include authentication technology.

105. On information and belief, one or more of the Dell-SAP '516 Products enable authenticating the identity of peer data objects.

106. On information and belief, the Dell-SAP '516 Products are available to businesses and individuals throughout the United States.

107. On information and belief, the Dell-SAP '516 Products are provided to businesses and individuals located in the Eastern District of Texas.

108. On information and belief, the Dell-SAP '516 Products enable first data objects to contain or be linked to a description of one or more peer data objects that are required to be connected to the first data object before the data object can be accessed by the peer data objects.

109. On information and belief, the Dell-SAP '516 Products enable the use of a digital signature that identifies the provider of a data object.

110. On information and belief, the Dell-SAP ‘516 Products contain systems and methods that comprise reading from a data object a description of one or more peer data objects that is required for use of the data object.

111. On information and belief, the Dell-SAP ‘516 Products contain functionality for determining whether the data object is authorized to communicate with one or more peer data objects.

112. On information and belief, the Dell-SAP ‘516 Products contain the capability to determine if the data object is authorized to communicate with one or more peer data objects.

113. On information and belief, the Dell-SAP ‘516 Products are capable of controlling the connection of the peer data objects to the data object.

114. On information and belief, the Dell-SAP ‘516 Products comprise systems and methods that connect a data object to peer data objects based upon authorization being granted. Moreover, when authorization is granted for the connection of a data object to peer data objects the peer data objects can communicate with the data object and the data object can communicate with the peer data objects.

115. On information and belief, the Dell-SAP ‘516 Products support authenticating a data object where the data object is encrypted.

116. On information and belief, Dell and SAP have directly infringed and continue to directly infringe the ‘516 patent by, among other things, making, using, offering for sale, and/or selling data object authentication and verification technology, including but not limited to the Dell-SAP ‘516 Products, which include infringing verification and authentication technologies. Such products and/or services include, by way of example and without limitation, the Dell SAP HANA Solution (incorporating the Dell PowerEdge R920 platform).

117. By making, using, testing, offering for sale, and/or selling authentication and verification products and services, including but not limited to the Dell-SAP ‘516 Products, Dell and SAP, acting as a joint enterprise and pursuant to ongoing contractual agreements, have

injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '516 patent, including at least claims 1, 17, and 20, pursuant to 35 U.S.C. § 271(a).

118. On information and belief, Dell and SAP also indirectly infringe the '516 patent by actively inducing infringement under 35 USC § 271(b).

119. On information and belief, Dell and SAP had knowledge of the '516 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Dell and SAP knew of the '516 patent and knew of its infringement, including by way of this lawsuit.

120. On information and belief, Dell and SAP intended to induce patent infringement by third-party customers and users of the Dell-SAP '516 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Dell and SAP specifically intended and were aware that the normal and customary use of the accused products would infringe the '516 patent. Dell and SAP performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '516 patent and with the knowledge that the induced acts would constitute infringement. For example, Dell and SAP provide the Dell-SAP '516 Products that have the capability of operating in a manner that infringe one or more of the claims of the '516 patent, including at least claims 1, 17, and 20, and Dell and SAP further provide documentation and training materials that cause customers and end users of the Dell-SAP '516 Products to utilize the products in a manner that directly infringe one or more claims of the '516 patent. By providing instruction and training to customers and end-users on how to use the Dell-SAP '516 Products in a manner that directly infringes one or more claims of the '516 patent, including at least claims 1, 17, and 20, Dell and SAP specifically intended to induce infringement of the '516 patent. On information and belief, Dell and SAP engaged in such inducement to promote the sales of the Dell-SAP '516 Products, *e.g.*, through Dell and SAP's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '516 patent. Accordingly, Dell and SAP have induced and continues to induce users of the accused products to use the accused products in their ordinary and customary

way to infringe the ‘516 patent, knowing that such use constitutes infringement of the ‘516 patent.

121. The ‘516 patent is well-known within the industry as demonstrated by the over 108 citations to the ‘516 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (e.g., LG Electronics, Inc. and Siemens AG). Several of Dell and SAP’s competitors have paid considerable licensing fees for their use of the technology claimed by the ‘516 patent. In an effort to gain an advantage over Dell and SAP’s competitors by utilizing the same licensed technology without paying reasonable royalties, Dell and SAP infringed the ‘516 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

122. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘516 patent.

123. As a result of Dell and SAP’s infringement of the '516 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Dell and SAP’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Dell and SAP together with interest and costs as fixed by the Court.

## COUNT IV
## INFRINGEMENT OF U.S. PATENT NO. 7,650,504

124. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

125. Dell designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for verifying the authenticity of executable images.

126. Dell designs, makes, sells, offers to sell, imports, and/or uses the Dell KACE K1000 Systems Management Appliance 6.4.120822; Dell KACE K1000 Systems Management Appliance 6.4.120756; Dell KACE K1000 Systems Management Appliance 6.4; Dell KACE K1000 Systems Management Appliance 6.3; Dell KACE K1000 Systems Management Appliance 6.2.109330; Dell KACE K1000 Systems Management Appliance 6.2.109329; Dell

KACE K1000 Systems Management Appliance 6.0.101863; Dell KACE K1000 Systems Management Appliance 5.590545; Dell KACE K1000 Systems Management Appliance 5.4.76847; and the Dell KACE K1000 Systems Management Appliance 5.4.70402 (collectively, the "Dell '504 Product(s)").

127. On information and belief, one or more Dell subsidiaries and/or affiliates use the Dell '504 Products in regular business operations.

128. On information and belief, one or more of the Dell '504 Products include authentication technology.

129. On information and belief, one or more of the Dell '504 Products comprise systems and methods for determining the authenticity of an executable image.

130. On information and belief, one or more of the Dell '504 Products enable authenticating and verifying an executable image. In particular, the Dell '504 Products determine whether a software application that has been dynamically connected to another data object has been tampered with subsequent to the execution of the software application.

131. On information and belief, the Dell '504 Products are available to businesses and individuals throughout the United States.

132. On information and belief, the Dell '504 Products are provided to businesses and individuals located in the Eastern District of Texas.

133. On information and belief, the Dell '504 Products enable the use of a reference digital signature for an executable image. The reference digital signature uses the contents of the executable image excluding portions of the executable that are fixed-up by a program loader.

134. On information and belief, the Dell '504 Products comprise a system wherein a reference digital signature is generated based on an executable image.

135. On information and belief, the Dell '504 Products generate a reference digital signature that excludes one or more locations in an executable image.

136. On information and belief, the Dell '504 Products comprise systems and methods wherein subsequent to the loading of the executable image the '504 Products determine an

authenticity digital signature to verify that the executable image has not been improperly modified.

137. On information and belief, the Dell '504 Products comprise systems and methods that generate an authenticity digital signature that excludes one or more locations in an executable image.

138. On information and belief, the Dell '504 Products are systems and methods that generate an authenticity digital signature after the executable image is loaded into memory. The authenticity digital signature which is generated by the Dell '504 Products excludes one or more pointers in need of fixing up;

139. On information and belief, the Dell '504 Products comprise systems and methods that determine whether the authenticity digital signature matches the reference digital signature.

140. On information and belief, the Dell '504 Products enable the generating of a reference digital signature prior to loading the executable image into memory. Specifically, the Dell '504 Products generate a reference digital signature that excludes one or more pointers from the reference digital signature.

141. On information and belief, the Dell '504 Products contain functionality wherein the digital signature is generated based on a first and second point in time.

142. On information and belief, the Dell '504 Products have the ability to compare the reference digital signature and the authenticity digital signature to perform an authenticity check.

143. On information and belief, the Dell '504 Products enable the detection of corrupted data in a computer image.

144. On information and belief, the Dell '504 Products enable the verification of the integrity of software images.

145. On information and belief, Dell has directly infringed and continues to directly infringe the '504 patent by, among other things, making, using, offering for sale, and/or selling content protection technology, including but not limited to the Dell '504 Products, which includes technology for verifying the authenticity of a software image. Such products and/or

services include, by way of example and without limitation, the Dell KACE K1000 Systems Management Appliance 6.4.120822; Dell KACE K1000 Systems Management Appliance 6.4.120756; Dell KACE K1000 Systems Management Appliance 6.4; Dell KACE K1000 Systems Management Appliance 6.3; Dell KACE K1000 Systems Management Appliance 6.2.109330; Dell KACE K1000 Systems Management Appliance 6.2.109329; Dell KACE K1000 Systems Management Appliance 6.0.101863; Dell KACE K1000 Systems Management Appliance 5.590545; Dell KACE K1000 Systems Management Appliance 5.4.76847; and the Dell KACE K1000 Systems Management Appliance 5.4.70402.

146. By making, using, testing, offering for sale, and/or selling authentication and verification technologies and services, including but not limited to the Dell '504 Products, Dell has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '504 patent, including at least claims 1 and 10, pursuant to 35 U.S.C. § 271(a).

147. On information and belief, Dell also indirectly infringes the '504 patent by actively inducing infringement under 35 USC § 271(b).

148. On information and belief, Dell had knowledge of the '504 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Dell knew of the '504 patent and knew of its infringement, including by way of this lawsuit.

149. On information and belief, Dell intended to induce patent infringement by third-party customers and users of the Dell '504 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Dell specifically intended and was aware that the normal and customary use of the accused products would infringe the '504 patent. Dell performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '504 patent and with the knowledge that the induced acts would constitute infringement. For example, Dell provides the Dell '504 Products that have the capability of operating in a manner that infringe one or more of the claims of the '504 patent, including at least claims 1 and 10, and Dell further

provides documentation and training materials that cause customers and end users of the Dell '504 Products to utilize the products in a manner that directly infringe one or more claims of the '504 patent. By providing instruction and training to customers and end-users on how to use the Dell '504 Products in a manner that directly infringes one or more claims of the '504 patent, including at least claims 1 and 10, Dell specifically intended to induce infringement of the '504 patent. On information and belief, Dell engaged in such inducement to promote the sales of the Dell '504 Products, e.g., through Dell user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '504 patent. Accordingly, Dell has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '504 patent, knowing that such use constitutes infringement of the '504 patent.

150. The '504 patent is well-known within the industry as demonstrated by the over 30 citations to the '504 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Apple, Inc. and Electronics and Telecommunications Research Institute (ETRI)). Several of Dell's competitors have paid considerable licensing fees for their use of the technology claimed by the '504 patent. In an effort to gain an advantage over Dell's competitors by utilizing the same licensed technology without paying reasonable royalties, Dell infringed the '504 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

151. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '504 patent.

152. As a result of Dell's infringement of the '504 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Dell's infringement, but in no event less than a reasonable royalty for the use made of the invention by Dell together with interest and costs as fixed by the Court.

**COUNT V**
**INFRINGEMENT OF U.S. PATENT NO. 7,650,418**

153. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

154. Dell and F5 Networks, in a joint enterprise, make, use, sell, and/or offer for sale in the United States products and/or services for controlling the usage of digital objects.

155. Dell and F5 Networks, in a joint enterprise, design, make, sell, offer to sell, import, and/or use a joint solution, the F5 BIG-IP for Dell DX Object Storage Platform (the "Dell-F5 '418 Product(s)").

156. On information and belief, one or more Dell and F5 subsidiaries and/or affiliates use the Dell-F5 '418 Products in regular business operations.

157. On information and belief, one or more of the Dell-F5 '418 Products comprise systems and methods for intercepting a communication between two applications in a computer environment.

158. On information and belief, one or more of the Dell-F5 '418 Products enable intercepting a communication between two applications where the first and second application communicate via a predefined communications channel.

159. On information and belief, the Dell-F5 '418 Products are available to businesses and individuals throughout the United States.

160. On information and belief, the Dell-F5 '418 Products are provided to businesses and individuals located in the Eastern District of Texas.

161. On information and belief, the Dell-F5 '418 Products include systems and methods that comprise a discreet intercept technology component (DIT) and a dynamic connection logic component (DCL).

162. On information and belief, the Dell-F5 '418 Products comprise systems and methods wherein the DIT component permits the interception of communication and data flows between two or more components in component-based applications.

163. On information and belief, the Dell-F5 '418 Products enable the DIT component to be inserted between two digital components. The DIT then intercepts the data and communications, thereby controlling the communication between the two digital components.

164. On information and belief, the Dell-F5 '418 Products comprise systems and methods that enable a control object capable of specifying a dynamic control logic depending on the intercepted data communication.

165. On information and belief, the Dell-F5 '418 Products enable applying by the intercept application the dynamic control logic specified by the control object on the digital object.

166. On information and belief, the Dell-F5 '418 Products contain functionality for intercepting data communication between a first application and a second application within a computer network without changing the functionality of the first application and the second application.

167. On information and belief, Dell and F5 have directly infringed and continue to directly infringe the '418 patent by, among other things, making, using, offering for sale, and/or selling digital rights technology, including but not limited to the Dell-F5 '418 Products, which include infringing technology for controlling the usage of data objects. Such products and/or services include, by way of example and without limitation, the F5 BIG-IP for Dell DX Object Storage Platform.

168. By making, using, testing, offering for sale, and/or selling digital rights management products and services, including but not limited to the Dell-F5 '418 Products, Dell and F5, acting as a joint enterprise and pursuant to ongoing contractual agreements, have injured MOV Intelligence and are liable to MOV Intelligence for directly infringing one or more claims of the '418 patent, including at least claims 1, 2, 4, 7, 8, and 9, pursuant to 35 U.S.C. § 271(a).

169. On information and belief, Dell and F5 also indirectly infringe the '418 patent by actively inducing infringement under 35 USC § 271(b).

170. On information and belief, Dell and F5 had knowledge of the ‘418 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Dell and F5 knew of the ‘418 patent and knew of its infringement, including by way of this lawsuit.

171. On information and belief, Dell and F5 intended to induce patent infringement by third-party customers and users of the Dell-F5 ‘418 Products and had knowledge that the inducing acts would cause infringement or were willfully blind to the possibility that their inducing acts would cause infringement. Dell and F5 specifically intended and were aware that the normal and customary use of the accused products would infringe the ‘418 patent. Dell and F5 performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘418 patent and with the knowledge that the induced acts would constitute infringement. For example, Dell and F5 provided the Dell-F5 ‘418 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘418 patent, including at least claims 1, 2, 4, 7, 8, and 9, and Dell and F5 further provide documentation and training materials that cause customers and end users of the Dell-F5 ‘418 Products to utilize the products in a manner that directly infringes one or more claims of the ‘418 patent. By providing instruction and training to customers and end-users on how to use the Dell-F5 ‘418 Products in a manner that directly infringes one or more claims of the ‘418 patent, including at least claims 1, 2, 4, 7, 8, and 9, Dell and F5 specifically intended to induce infringement of the ‘418 patent. On information and belief, Dell and F5 engaged in such inducement to promote the sales of the Dell-F5 ‘418 Products, *e.g.*, through Dell and F5 user manuals, product support, marketing materials, and training materials that actively induce the users of the accused products to infringe the ‘418 patent. Accordingly, Dell and F5 have induced and continue to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘418 patent, knowing that such use constitutes infringement of the ‘418 patent.

172. The ‘418 patent is well-known within the industry as demonstrated by the over 47 citations to the ‘418 patent family in issued patents and published patent applications assigned to

technology companies and academic institutions (*e.g.*, Google, Inc. and International Business Machines Corporation). Several of Dell and F5's competitors have paid considerable licensing fees for their use of the technology claimed by the '418 patent. In an effort to gain an advantage over Dell and F5's competitors by utilizing the same licensed technology without paying reasonable royalties, Dell and F5 infringed the '418 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

173. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '418 patent.

174. As a result of Dell and F5's infringement of the '418 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Dell and F5's infringement, but in no event less than a reasonable royalty for the use made of the inventions by Dell and F5 together with interest and costs as fixed by the Court.

## COUNT VI
## INFRINGEMENT OF U.S. PATENT NO. 7,124,114

175. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

176. Dell designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing the distribution of digital content and preventing unauthorized access to protected digital content.

177. Dell designs, makes, sells, offers to sell, imports, and/or uses the Dell SonicWALL SuperMassive E10800; Dell SonicWALL SuperMassive E10400; Dell SonicWALL SuperMassive E10200; Dell SonicWALL SuperMassive 9800; Dell SonicWALL SuperMassive 9600; Dell SonicWALL SuperMassive 9400; Dell SonicWALL SuperMassive 9200; Dell SonicWALL Network Security Appliance (NSA) 6600; Dell SonicWALL Network Security Appliance (NSA) 5600; Dell SonicWALL Network Security Appliance (NSA) 4600; Dell SonicWALL Network Security Appliance (NSA) 3600; Dell SonicWALL Network Security

Appliance (NSA) 2600; Dell SonicWALL Network Security Appliance (NSA) 250M Series; and the Dell SonicWALL Network Security Appliance (NSA) 220 Series (collectively, the "Dell '114 Product(s)").

178. On information and belief, one or more Dell subsidiaries and/or affiliates use the Dell '114 Products in regular business operations.

179. On information and belief, one or more of the Dell '114 Products include content protection and content access technology.

180. On information and belief, one or more of the Dell '114 Products enable providing or withholding access to digital content is accordance with digital rights management protection terms.

181. On information and belief, the Dell '114 Products are available to businesses and individuals throughout the United States.

182. On information and belief, the Dell '114 Products are provided to businesses and individuals located in the Eastern District of Texas.

183. On information and belief, the Dell '114 Products enable the distribution of protected digital data.

184. On information and belief, the Dell '114 Products comprise systems and methods wherein the Dell '114 Products ascertain terms for providing protected data to a prospective requestor according at least in part to information of unauthorized copying of other protected material previously provided to said prospective requestor.

185. On information and belief, the Dell '114 Products comprise systems and methods that provide authorization to allow access or deny access to protected digital data based on ascertained terms.

186. On information and belief, Dell has directly infringed and continues to directly infringe the '114 patent by, among other things, making, using, offering for sale, and/or selling digital content protection technology, including but not limited to the Dell '114 Products, which include infringing digital rights management technologies. Such products and/or services

include, by way of example and without limitation, the Dell SonicWALL SuperMassive E10800; Dell SonicWALL SuperMassive E10400; Dell SonicWALL SuperMassive E10200; Dell SonicWALL SuperMassive 9800; Dell SonicWALL SuperMassive 9600; Dell SonicWALL SuperMassive 9400; Dell SonicWALL SuperMassive 9200; Dell SonicWALL Network Security Appliance (NSA) 6600; Dell SonicWALL Network Security Appliance (NSA) 5600; Dell SonicWALL Network Security Appliance (NSA) 4600; Dell SonicWALL Network Security Appliance (NSA) 3600; Dell SonicWALL Network Security Appliance (NSA) 2600; Dell SonicWALL Network Security Appliance (NSA) 250M Series; and the Dell SonicWALL Network Security Appliance (NSA) 220 Series.

187. By making, using, testing, offering for sale, and/or selling digital rights management and access control products and services, including but not limited to the Dell '114 Products, Dell has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '114 patent, including at least claims 1, 21, 41, and 52, pursuant to 35 U.S.C. § 271(a).

188. On information and belief, Dell also indirectly infringes the '114 patent by actively inducing infringement under 35 USC § 271(b).

189. On information and belief, Dell had knowledge of the '114 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Dell knew of the '114 patent and knew of its infringement, including by way of this lawsuit.

190. On information and belief, Dell intended to induce patent infringement by third-party customers and users of the Dell '114 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Dell specifically intended and was aware that the normal and customary use of the accused products would infringe the '114 patent. Dell performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '114 patent and with the knowledge that the induced acts would constitute infringement. For example, Dell provides the Dell '114 Products that have the capability of operating in a manner that infringe

one or more of the claims of the ‘114 patent, including at least claims 1, 21, 41, and 52, and Dell further provides documentation and training materials that cause customers and end users of the Dell ‘114 Products to utilize the products in a manner that directly infringe one or more claims of the ‘114 patent. By providing instruction and training to customers and end-users on how to use the Dell ‘114 Products in a manner that directly infringes one or more claims of the ‘114 patent, including at least claims 1, 21, 41, and 52, Dell specifically intended to induce infringement of the ‘114 patent. On information and belief, Dell engaged in such inducement to promote the sales of the Dell ‘114 Products, e.g., through Dell user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘114 patent. Accordingly, Dell has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘114 patent, knowing that such use constitutes infringement of the ‘114 patent.

191. The ‘114 patent is well-known within the industry as demonstrated by the over 39 citations to the ‘114 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Aigo Research Institute of Image Computing Co., Ltd. and General Electric Company). Several of Dell’s competitors have paid considerable licensing fees for their use of the technology claimed by the ‘114 patent. In an effort to gain an advantage over Dell’s competitors by utilizing the same licensed technology without paying reasonable royalties, Dell infringed the ‘114 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

192. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘114 patent.

193. As a result of Dell’s infringement of the '114 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Dell’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Dell together with interest and costs as fixed by the Court.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff MOV Intelligence respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff MOV Intelligence that Dell has infringed, either literally and/or under the doctrine of equivalents, the '230 patent, the '006 patent, the '504 patent, and the '114 patent;

B. A judgment in favor of Plaintiff MOV Intelligence that Dell and SAP have jointly infringed in a joint enterprise and pursuant to ongoing contractual agreements between Dell and SAP, either literally and/or under the doctrine of equivalents, the '516 patent;

C. A judgment in favor of Plaintiff MOV Intelligence that Dell and F5 Networks have jointly infringed in a joint enterprise and pursuant to ongoing contractual agreements between Dell and F5 Networks, either literally and/or under the doctrine of equivalents, the '418 patent;

D. An award of damages resulting from Defendants' acts of infringement in accordance with 35 U.S.C. § 284;

E. A judgment and order finding that Defendants' infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiff enhanced damages.

F. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees against Defendants.

G. Any and all other relief to which MOV Intelligence may show itself to be entitled.

## JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, MOV Intelligence requests a trial by jury of any issues so triable by right.

Dated: September 30, 2016

Respectfully submitted,

/s/ Dorian S. Berger _____

Elizabeth L. DeRieux (TX Bar No. 05770585)
D. Jeffrey Rambin (TX Bar No. 00791478)
CAPSHAW DERIEUX, LLP
114 E. Commerce Ave.
Gladewater, Texas 75647
Telephone: 903-236-9800
Facsimile: 903-236-8787
E-mail: ederieux@capshawlaw.com
E-mail: jrambin@capshawlaw.com

OF COUNSEL:

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
BERGER & HIPSKIND LLP
1880 Century Park East, Ste. 815
Los Angeles, CA 95047
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com

*Attorneys for Marking Object Virtualization Intelligence, LLC*